

Pre



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/738,807	12/13/2000	Jeremy Lawrence	81862.P178	2439
7590 10/21/2004			EXAMINER	
Sang Hui Michael Kim BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP 7th Floor 12400 Wilshire Boulevard Los Angeles, CA 90025-1026			FLEMING, FRITZ M	
			ART UNIT	PAPER NUMBER
			2182	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/738,807

Applicant(s)

LAWRENCE, JEREMY

Examiner

Fritz M Fleming

Art Unit

2182

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-46 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

*Fritz M. Fleming*  
FRITZ FLEMING  
PRIMARY EXAMINER  
GROUP 2100

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5, 11-15, 16-21, 22-31, 32-41 and 42-46 are rejected under 35

U.S.C. 102(e) as being anticipated by Arrow et al. '917 (Arrow).

Per Figure 1, a VPN includes 115-155 and VPN management station 160. To manage the configuration or reconfiguration of VPN unit 115 (i.e. a network device) via 160 per Figure 11, for example, the management traffic is sent from 160 to 115 over the VPN itself.

Therefore, the method of claim 1 comprises the receiving of management traffic over the VPN, wherein the managed network device 115 uses the traffic received over the VPN from station 160. Per claim 2, the managing includes managing network device 115 using secure in-band management due to the use of at least the encryption of column 7. Per claim 3, a one or more management port 414 is linked with the VPN for management thereof. Per claim 4, a management function (i.e. Figures 5 and 6) internal to 115 is linked with the VPN via the schematic of Figure 4. Per claim 5, IP services are carried out via column 7.

Similarly, the claim 11-15 method steps are met by configuring VPN unit 115 to support a VPN via section 160 and linking a management device 160 and its function with the VPN. Per claim 12, the management traffic is carried over the VPN itself. Per claim 13, the network device 115 is managed using the VPN carried management traffic. Per claim 14, the VPN is linked to the management device 160 at, for example, the interface 908 connecting 160 to 100. Per claim 15, IP services are carried out, *supra*.

The network device claims of 16-21 are anticipated via the following interpretation. The VPN unit 115, per columns 6-7, performs data traffic routing, and thus has a routing and forwarding module to forward packets for the network device, and thus configures the network device 115 to support a VPN, with a link that links a management function with the VPN via port 414. Per claim 17, the routing and forwarding module delivers management traffic on the VPN for the network device 115. Per claim 18, for example, a management module in 115 is seen as the configuration data in storage memory 408 when VPN 115 is configured or re-configured by station 160 as set forth by column 10. Per claim 19, an external link at port 414 links the device 115 to the VPN. Per claim 20, an internal link via 602 and 408 links the VPN to the management function 602 and 408 internal to the network device 115 per Figures 4-6. Per claim 21, IP services are addressed *supra*.

The claim 22-26 "means+function" are met by the means for receiving management traffic over the VPN, at for example, 414, and means for managing the network device using the management traffic received over the VPN, at for example, at

Art Unit: 2182

Figures 4-6. Means for secure in-band management are the encryption, supra. Means for linking one or more management ports 414 of VPN 115 with the VPN are seen in Figure 4 at the "to 100". Means of Figures 4-6 link the internal management function with the VPN. Means perform IP services, supra. These claims parallel 1-5.

The claim 27-31 "means+function" claims parallel claims 11-15, and thus set forth a means for configuring a network device 115 by station 160 to support a VPN, with means linking the management device 160 and its functionality to the VPN via port 908. The various portion of the VPN and its constituent items set forth the means for carrying the management traffic over the VPN. Means for managing the network device are seen at Figures 4-6 to manage 115 using the management traffic over the VPN. Means link the VPN to the management device 160 at port 908 using an external link. IP services are carried out by the means of the VPN and network itself, supra.

Per claims 32-41, machine-readable medium is present to carry out the above functions via the computer based VPN.

Per claims 42-46, note Figure 1 which shows one or more devices 115 and the like to configure the VPN with one link to link the VPN to the management device 160, the management device 160 facilitating management of the network devices by sending management traffic over the VPN itself via the link thereto. Secure in-band management is attained via the encryption, supra. The network devices are connected via a port to the VPN, supra. Internal management functions link with the VPN, supra. IP services are carried out, supra.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow in view of applicant's admitted prior art (APA).

Arrow sets forth a substantial portion of the claimed subject matter via the anticipation analysis above. The analysis above shows a routing and forwarding module to route and forward data on single input and output links to configure the VPN and to receive management traffic over the VPN with a management module to receive management traffic from the VPN and to manage accordingly.

APA shows a plurality of input and output data links in Figure 4, with a plurality of VPN data input/output links at 422A-C. The purpose of these is to facilitate private communications on the particular router or the same modules on other routers.

Therefore it would have been obvious to one having ordinary skill in the art at the time that the invention was made to modify a VPN unit 115 per the teachings of the APA Figure 4 so that it is possible to facilitate private communications on the particular router or the same modules on other routers. As Arrow has shown the limitations of claims 7-10, the same analysis applies to the combined configuration of multiple input and output data links.

### ***Response to Arguments***

Applicant's arguments filed 9/20/2004 have been fully considered but they are not persuasive. Applicant repeats over and over that Arrow does not support any inference that management traffic is sent over the VPN. Applicant repeats that the VPN Management Station 160 is connected to the Public Network 100, without transmitting management traffic over the VPN. Applicant seems to believe that Arrow is only for configuring VPN units for use on a VPN prior to creation of the VPN via the public network. In other words, applicant seems to believe that Arrow configures VPN units over the public network prior to creation of the VPN itself. The examiner respectfully disagrees.

Before rebutting arguments made, a brief review of Arrow is in order. Arrow teaches that the use of VPNs on top of public networks, such as the Internet, is well known. Furthermore, a VPN unit ensures that secure communications between members of the same VPN. See column 2, lines 19-33. Thus this passage clearly teaches that VPNs are built on public networks and VPN units allow for secure communications on an existing VPN. Further evidence of the VPN unit being on an

existing VPN is found at column 3, lines 2-20. It is explicitly set forth that "One embodiment of the present invention is used in a virtual private network operating over a public data network. In this first embodiment, a virtual private network (VPN) unit within the virtual private network contains a processor and multiple storage memories for the storage of operating system programs." Thus it is clear that the present invention involves VPN management on an existing VPN operating over a public data network. The Brief Description of Figure 2 describes a packet transmitted over the public network from one member of a VPN to another member of the VPN, again emphasizing the use of an existing VPN to transmit packets. Thus turning to Figure 1 and its description, it is clear that the VPN comprises a VPN built over the public network to include the public network 100, the VPN units 115,125,135,145,155 operating under the control of the VPN management station 160. See column 5, lines 50+. "The VPN management station 160 controls VPN units 115,125,135 through commands and configuration information transmitted to the respective VPN unit through the public network 100." See column 6, lines 31+, which further shows that the management is carried out over the VPN built over the public network, as the VPN units are part of the VPN, as is the management station. The bottom of column 6, lines 55+ clearly illustrate that management is carried out over the VPN, as data traffic is routed through the VPN units, and each VPN unit maintains lookup tables for identifying members of specific virtual private network groups, to ensure that secure data communications between end users is achieved in a manner transparent to the users (column 7, lines 1-12). Figure 2 shows how a packet is transmitted over the VPN from



Art Unit: 2182

one VPN unit to another. Especially note, that if the source and destination address for the data packet are not members of the same VPN, then the packet is forwarded to the Internet as ordinary Internet traffic, as though the VPN unit were not involved. This is clear evidence that packets sent between VPN units are carried over the VPN, otherwise the traffic is considered to be ordinary Internet traffic. See column 7, lines 26+. Figure 3 and column 8, lines 21+, detail that Figure 3 shows how VPN traffic is carried over the VPN over the public data network. Line 32-35 even use the term "VPN traffic" when differentiating traffic sent over the VPN as opposed to normal Internet data traffic. Figure 4 details a VPN unit. Figure 5 shows storage memory, making express mention that the VPN unit 115 can be rebooted by a command received from the VPN management station 160 through the network port 414. As added security, the VPN unit 115 and management station 160 authenticate themselves to each other, to prevent corruption (see column 9, lines 18-25). Figure 6 includes configuration data 602 to operate VPN unit 115 to include being updated, configured, or reconfigured by the VPN management station 160, per column 9, lines 32-45. Referring back to Figure 4, the pointer 412 can be redirected in response to a command from the management station 160 per column 10, lines 1-15. A VPN unit reboot can be commanded by the VPN management station 160, per column 10, lines 24-40. Column 10, lines 41-51 explicitly state that the VPN unit 115 is configured or reconfigured by VPN management station 160, so as to ensure that VPN unit 115 continues to operate during the configuration or reconfiguration. Figure 7 details the operating system 116 of a VPN unit 115, such that column 11, lines 5-11 specify that communications within a VPN are encrypted before

Art Unit: 2182

being transmitted across public network 100, further proving that the VPN is operating over the public network 100, with the VPN traffic carried across the public network 100 via the VPN units and management station. Column 12, lines 1-10 detail configuration information that can be loaded from the VPN management station 160. Column 12, lines 21+ clearly specify how a VPN unit is configured and what "configuring" can encompass. When "configuring a VPN" a new VPN can be set up, an existing VPN can be edited, or a VPN can be deleted. See lines 28-33. Thus in order for an existing VPN to be edited or deleted, a VPN has to exist, thus requiring that any information transferred between VPN Units and the Management Station be transferred over the VPN itself, as non-VPN traffic is regarded and treated as regular Internet traffic and routed accordingly. Per lines 34+, it is clear that the network communication port 414 of the VPN unit 115 is monitored to detect configuration requests from the management station 160. Figure 8 shows how a new operating system is installed on a VPN unit 115 per a request from the VPN management station 160. Figure 9 shows how the VPN management station 160 is structured, to include the database 906 of the supported VPNs, see column 13, lines 50-67. Figure 10 and column 14, lines 1+ show how the communications library 1010 is used to communicate configuration information to the VPN units across network 100. Turning to Figure 12, one finds at column 15, lines 1+ that the lower level addressing for the VPN units is automatically generated by the management station 160. A VPN unit object 1200 is created for each VPN unit on the network, the network meaning the virtual private network. A VPN object 1220 is created for each virtual private network supported by the VPN management station 160, to

Art Unit: 2182

include a number of attributes like list of groups and remote clients. Figures 13 and 14 represent flow charts for creating a VPN and a group. As the VPN itself is built over the public network 100 and communications between VPN units is via the VPN built over the network, it is clear that any communications between VPN units and the management station be carried over the VPN itself. Thus the “management” or “configuration” of existing VPN units by the management station 160 clearly involves and requires the use of the VPN over the public network, and the VPN traffic is carried over the VPN itself, as Arrow has made it clear to distinguish between VPN traffic carried over the VPN built on the public network and regular Internet traffic that is not carried over the VPN. To conclude otherwise simply is not a proper reading of the Arrow reference in its entirety.

**102 Rejections over Arrow**

Claim 1: The examiner has made a clear showing above how the “configuration” of an existing VPN unit by the management station 160 requires that the traffic be carried over the VPN, as non-VPN traffic is treated as regular Internet traffic and routed accordingly. Thus the use of the public network is not as applicant has argued, as Arrow has built the VPN over the public network, thus the management traffic is carried over the VPN that is built on the public network. Applicant has misinterpreted the significance of the public network in the Arrow reference. Arrow has clearly provided more than an inference that management traffic is sent over the VPN, as Arrow clearly teaches that all VPN traffic is carried over the VPN built over the public network. Furthermore, the editing or deleting of an existing VPN unit (called a “configuration”

Art Unit: 2182

above) is not the creation of a VPN from scratch as argued by applicant, and thus the VPN management traffic is carried over the existing VPN. If applicant is trying to distinguish the claim by reading into such that a VPN is configured from scratch via the VPN itself, then the claims need further limitations to mean such.

Claim 2: How can the management station of a VPN not be a part of the VPN, when only VPN traffic is allowed to travel over the VPN itself? Thus the management station 160 is a part of the VPN and uses the VPN to send the management traffic destined for VPN units on the VPN.

Claim 3: Applicant is again not allowing for the fact that the VPN is built over the public network, thus an interface to the public network is required in order to realize the VPN over the public network.

Claim 4: Figure 4 again shows the use of the public network to link management to the management station 160 via the VPN over the public network 100.

Claim 5: no substantial argument to respond to.

Claim 11: Applicant is improperly limiting Arrow to the case in which a VPN is established from scratch (i.e. as discussed above related to Figure 13). However, the examiner has clearly pointed out above that Arrow does include "configuration" of existing VPN units on an existing VPN, thus all traffic, including the management traffic, is carried over the VPN that is built on the public network, as Arrow has clearly delineated between VPN traffic and regular Internet traffic. Thus all VPN traffic in an existing VPN is carried over the VPN, to include any and all management traffic from the management station 160. Applicant is unfairly limiting Arrow to the establishing of a

Art Unit: 2182

VPN from scratch, but Arrow clearly teaches the “configuring” of existing VPN units on existing VPNs also. The claim is very broad, only requiring that the network device be configured to support a VPN (any VPN unit is configured to do so), and a linking a management device or function with the VPN (management station 160 is linked to the VPN and provides management functionality).

Claim 13: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 14: no substantial argument presented.

Claim 15: no substantial argument presented.

Claim 16: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 17: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 18: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 19: no substantial argument presented.

Claim 20: no substantial argument presented.

Claim 21: no substantial argument presented.

Claim 22: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 23: The VPN management station 160 is a part of the VPN, or else it could not communicate with the VPN units, as non-VPN traffic is treated as regular

Art Unit: 2182

Internet traffic and not routed along the VPN. Encryption is used per columns 6-7 in which the data packet is properly encrypted, ensuring that the packet is being propagated between members of the same VPN.

Claim 24: no substantial argument presented.

Claim 25: no substantial argument presented.

Claim 26: no substantial argument presented.

Claim 27: VPN management station 160 has to be linked to the VPN in order to manage the VPN units, as a distinction has been made between VPN and regular Internet traffic. The claim does not actually require that the management function be carried over the VPN itself, just that there be a linking with the VPN.

Claim 28: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 29: Again, applicant incorrectly limits Arrow to the creation of a VPN, and not the management of an existing VPN, which is set forth in detail above.

Claim 30: no substantial argument presented.

Claim 31: no substantial argument presented.

Claims 32-41: see claims 1-5 and 11-15 above, with no additional argument provided.

Claim 42: Applicant fails to appreciate the fact that the VPN of Arrow is built over the public network, per the above analysis. Clearly, the VPN of Arrow includes the public network 100, as the VPN is built over the public network 100. Thus the VPN units are the one or more network devices "to configure a VPN", wherein the "to

Art Unit: 2182

configure” is a latent capability without any details regarding the actual manner in which the VPN is ultimately configured. The one or more links are clearly shown in Figure 1, as the VPN is linked to the management station 160, which facilitates management of the VPN units via the VPN itself, as the distinction has been clearly made between VPN and regular Internet traffic.

Claim 43: VPN management station 160 is a part of the VPN, with secure communications per columns 6 and 7.

Claim 44: As the port 414 is linked to the public network 100, it is linked to the VPN as the VPN is built over the public network.

Claim 45: no substantial argument presented.

Claim 46: no substantial argument presented.

**103 Rejection over Arrow in view of APA**

Claims 6-10: The combination proposed by the examiner does enhance the functionality of Arrow, as the APA adds a plurality of links, wherein Arrow has a single link. Figure 7 shows the configuration module 710 of the operating system 116 which manages the configuration of the VPN unit 115. The configuration module 710 responds to configuration requests or commands from the management station 160, and also reports configuration status information to the management station 160. Thus the configuration module 710 is a part of the VPN unit and manages the VPN unit in response to management traffic carried over the VPN. Applicant again unfairly limits Arrow to the creation of a VPN from scratch, not considering Arrow's explicit teachings

regarding the configuration and management of VPN units on an existing VPN. As pointed out above, Arrow does show a management module 710.

Having rebutted all arguments made by applicant, the rejection is made final.

***Conclusion***

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

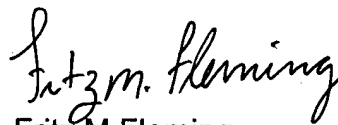
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fritz M Fleming whose telephone number is 571-272-4145. The examiner can normally be reached on M-F, 0600-1500.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin can be reached on 571-272-4146. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Art Unit: 2182

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Fritz M Fleming  
Primary Examiner  
Art Unit 2182

fmf